

## **Exhibit 7**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**22 MAG 1353**IN RE APPLICATION OF THE UNITED  
STATES OF AMERICA FOR ORDER TO  
DISCLOSE NON-CONTENT INFORMATION  
PURSUANT TO 18 U.S.C. § 2703(d)SEALED APPLICATION

Nicolas Roos affirms as follows:

1. I am an Assistant United States Attorney in the Southern District of New York and, as such, I am familiar with this matter.

2. The Government is seeking an Order pursuant to Title 18, United States Code, Section 2703(d) to require Google, LLC, Oath Holdings Inc., and Microsoft Corporation (the “Providers”), to provide the to/from headers and other non-content information for e-mails stored in the following email accounts (the “Target Accounts”):

Email Address	Provider	Target Account #
patorlando1@gmail.com	Google, LLC	Target Account-1
porlando@benesserecapital.com	Google, LLC	Target Account-2
porlando@beneinvest.com	Google, LLC	Target Account-3
porlando@dwacspac.com	Google, LLC	Target Account-4
bjg@garelickcapital.com	Google, LLC	Target Account-5
bruce328i@yahoo.com	Oath Holdings Inc.	Target Account-6
mshvartsman71@gmail.com	Google, LLC	Target Account-7
gerald@sourceoutdoor.net	Google, LLC	Target Account-8
gerald@sourcefurniture.com	Google, LLC	Target Account-9
allenjbeyer@gmail.com	Google, LLC	Target Account-10
apost82@gmail.com	Google, LLC	Target Account-11
adrill1@gmail.com	Google, LLC	Target Account-12

adrill1@hotmail.com	Microsoft Corporation	Target Account-13
javill1961@gmail.com	Google, LLC	Target Account-14

The records requested from the Providers are set forth below and in the accompanying proposed Order.

3. 18 U.S.C. § 2703(c) provides authority for a court to order an electronic communications service provider to disclose records or information not including the contents of communications without notice to the subscriber or customer, if the records are relevant and material to an ongoing criminal investigation.

4. Specifically, 18 U.S.C. § 2703(c)(1) provides in pertinent part:

A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or a customer of such service (not including the contents of communications) . . . when the governmental entity—

....

obtains a court order for such disclosure under subsection (d) of this section;

....

5. 18 U.S.C. § 2703(d), in turn, provides (in pertinent part):

A court order for disclosure under subsection . . . (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.

As specified in 18 U.S.C. § 2711(3), this Court is a court of competent jurisdiction under the Stored Communications Act because it has jurisdiction over the offenses being investigated, as defined below.

6. In addition, 18 U.S.C. § 2703(c)(3) provides:

A governmental entity receiving records or information under [18 U.S.C. § 2703(c)] is not required to provide notice to a subscriber or customer.

7. Finally, 18 U.S.C. § 2705(b) authorizes the Court to issue an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b)(1)-(5).

The Requested Records are Relevant and Material to an Ongoing Investigation

8. On or about February 10, 2022, the United States Attorney’s Office submitted a search warrant application to the Honorable Debra Freeman to search the contents of five Apple iCloud accounts and three Google email accounts, based on facts set forth in the affidavit of Special Agent Marc Troiano of the Federal Bureau of Investigation. The affidavit of Special Agent Troiano was submitted at the same time as this application and is incorporated herein by reference. The affidavit describes probable cause to believe that certain target subjects of the investigation have engaged in insider trading and/or made false statements to the United States Securities and Exchange Commission (“SEC”), in violation of Title 18, United States Code, Sections 2, 371, 1001, 1343, 1348, 1349 and Title 15, United States Code, Sections 77x, 78j(b) and 78ff and Title 17, Code of Federal Regulations, Section 240.10b-5 (collectively, the “Subject Offenses”).

9. Specifically, as described in the affidavit, the FBI and the United States Attorney's Office for the Southern District of New York are investigating an insider trading scheme in securities of Digital World Acquisition Corporation ("DWAC"), a special purpose acquisition company ("SPAC")<sup>1</sup>, the shares of which were publicly traded on the Nasdaq stock market beginning on or about September 3, 2021. On or about October 20, 2021, DWAC and Trump Media & Technology Group ("Trump Media"), a media and technology company founded in February 2021 by former United States President Donald J. Trump, announced that they had entered into a definitive merger agreement that would combine the two entities, allowing Trump Media to become a publicly-traded company. The investigation relates to disclosures in public filings by DWAC, as well as trading in DWAC stock in September and October 2021 based on material non-public information about its planned merger with Trump Media. As set forth in the affidavit, there is probable cause to believe that Patrick Orlando, the chief executive officer of DWAC, made false statements in filings with the SEC by falsely stating that DWAC was not in negotiations with any SPAC target, even though DWAC was in negotiations with Trump Media and other entities at the time. Additionally, as described in the affidavit, there is probable cause to believe that Bruce Garelick, a DWAC director, and other individuals who appear to be affiliated with or known to Garelick – including Michael Shvartsman, Gerald Shvartsman, Allen Beyer, Anton Postolnikov, Adrian Lopez Torres, and Javier Lopez Lopez – purchased DWAC stock after learning non-public information about its planned merger with Trump Media, and sold the stock shortly after the merger was announced.

---

<sup>1</sup> A special purpose acquisition company, also known as a "blank check company," is a publicly traded company created for the purpose of acquiring or merging with an existing private company, thus making it public without going through the traditional initial public offering process.

10. The requested records relating to the Target Accounts are relevant and material to an ongoing investigation. First, according to information provided by DWAC's outside counsel to the SEC, Patrick Orlando used Target Account-1, Target Account-2, Target Account-3, and Target Account-4 to email about matters relating to DWAC, and therefore there are reasonable grounds to believe that the requested information for those Target Accounts will reveal who Orlando was emailing with at times relevant to the insider trading investigation. Second, Target Account-5 and Target Account-6 belong to Bruce Garelick. As set forth in the attached affidavit, Garelick appears to have provided material non-public information about DWAC's business combination with Trump Media to other individuals. Target Account-5 is associated with Garelick's Apple account and is in the name of his business. Target Account-6 is associated with Garelick's AT&T account. There are reasonable grounds to believe that the requested information for Target Account-5 and Target Account-6 will reveal whether Garelick used those email accounts to communicate with co-conspirators in the insider trading scheme, or to receive information about DWAC. Third, Target Account-7 through Target Account-14 appear to be used by individuals who may have traded on the basis of material non-public information about DWAC. Based on publicly available information from LinkedIn, Target Account-7 appears to be used by Michael Shvartsman. Based on information from Apple, Target Account-8 and Target Account-9 appear to be used by Gerald Shvartsman. Based on publicly available information from LinkedIn, Target Account-10 appears to be used by Allen Beyer. Based on information from Apple, Target Account-11 appears to be used by Anton Postolnikov, Target Account-12 and Target Account-13 appear to be used by Adrian Lopez Torres, and Target Account-14 appears to be used by Javier Lopez Lopez. There are reasonable grounds to believe that the requested information for Target Account-7 through Target Account-14 will reveal whether the account users communicated with Garelick and/or other individuals who had non-public information about DWAC. Additionally, those Target Accounts

are likely to provide information about the Target Subjects' trading activity, including emails from brokerages or banks.

11. In addition to header information, the Government also requests device information, IP address information, and cookie and linked account information for each of the Target Accounts. Specifically:

a. *Device information:* Google frequently obtains information about the types of devices that are used to access accounts like the Target Accounts. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the Provider to keep track of the devices using its services. Those device identifiers include GUIDs or Global Unique Identifiers, phone numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). These device identifiers can then be used (a) to determine the other accounts that are accessed by the same device and thus likely by the same person at the Provider tracking that information, (b) to determine accounts accessed at other providers by that same device, (c) to determine whether any physical devices found in the course of the investigation were the ones used to access each of the Target Accounts.

b. *IP address information:* An IP address is generally used to route communications between a Provider and the Target Accounts. Providers of certain communication

services also require the use of additional routing information to accompany message or other communication in order to route information to the user of a certain account. That is commonly referred to as “network address translation,” which allows information traveling, for example, to a particular household to reach the correct device within that household; this is sometimes accomplished by assigning a particular “port” for communications going between a Provider and the Target Accounts. Large mobile telephone carriers sometimes use more sophisticated systems that are referred to as “carrier grade” network address translation. The network address translation information is relevant because it will assist the investigation in resolving which account on, for example, a mobile carrier was used to send and receive information between the Target Accounts and a Provider, which can then assist in identifying whose cellular telephone was being used when accessing the Target Accounts.

c. *Cookie and linked account information:* Google often use features to track the activity of users of its accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account like one of the Target Accounts. As noted above, one of the ways it does that is by using cookies. Because one of the purposes of the investigation is to determine all of the accounts and means of communication used by the subjects of the investigation, both to identify the subjects and to obtain evidence of their conduct under investigation, the order calls for Google to provide records sufficient to identify those other accounts.

12. Based on the foregoing, the Government requests that the Court enter the proposed Order submitted herewith. The materials to be requested from the Target Accounts will be limited, to the extent they are dated, to those created, sent, received, modified, or deleted on or about December 11, 2020, for the reasons set forth in the affidavit.

Non-Disclosure and Sealing



13. The Government further requests, pursuant to 18 U.S.C. § 2705(b), that this Application and the proposed Order be sealed by the Court until such time as the Court directs otherwise, and that the Provider be ordered not to notify any person (including the subscriber associated with the Target Account) of the existence of the Order for a period of one year from the date of the Order, subject to extension if necessary. In this case, such an order would be appropriate because the attached Order concerns an ongoing criminal investigation, where the existence and scope of the investigation is not known to the targets of the investigation, the account holders are suspected of being involved in or associated with persons involved in the conduct under investigation, and disclosure of Order to the account owner or to any other person may alert subjects or targets of the ongoing investigation. The targets of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3). Moreover, certain of the targets are believed to travel internationally frequently. *See* 18 U.S.C. §§ 2705(b)(2), (5). Accordingly, there is reason to believe that notification of the existence of the attached Order will seriously jeopardize the investigation, including by giving targets an opportunity to flee or avoid prosecution, or tamper with evidence, including electronically stored information that is easily tampered with. Given the amount of time a criminal investigation commonly lasts and the particular circumstances presented here, the Government respectfully submits that one year is an appropriate delay of notice period for the Court to order.


14. I know from past experience that Google will request that the Government seek data related email addresses with an enterprise domain such as, @benesserecapital.com, @beneinvest.com, @dwacspac.com, @garelickcapital.com, and @sourceoutdoor.net, which would include data relating to five of the Target Accounts, directly from the enterprises, pursuant

to the U.S. Department of Justice Policy titled Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at <https://www.justice.gov/criminal-ccips/file/1017511/download>. However, @benesserecapital.com, @beneinvest.com, @dwacspac.com, @garelickcapital.com, @sourcefurniture.com and @sourceoutdoor.net appears to be owned or controlled by Patrick Orlando, Bruce Garelick, and Gerald Shvartsman, respectively, all of whom are Target Subjects of this investigation. As they are the apparent owners of the enterprises, or are involved in controlling them (as is the case with Orlando with DWAC), notification would almost certainly mean they would be informed of the existence of this search warrant, which could cause them to delete, encrypt, or otherwise conceal the requested data. To the extent the enterprises have outside counsel, disclosure to outside counsel does not appear to be a viable option because, based on my understanding of professional responsibility rules, such counsel will be required to report such a disclosure to the client. Additionally, it is my understanding that certain materials requested from Google cannot be obtained directly from the enterprise because enterprise account users cannot access or download certain types of data, including the types of data requested for the Target Accounts. Therefore, I respectfully request that the proposed order specifically require the Provider to produce enterprise data.

15. No prior request for the relief sought herein has been made.

16. I declare under penalty of perjury that the foregoing factual assertions are true and correct to the best of my knowledge and belief.

Dated: New York, New York  
February 10, 2022

  
\_\_\_\_\_  
Nicolas Roos  
Assistant United States Attorney  
212-637-2421